Distribution of Artin-Schreier Extensions

Thorsten Lagemann[*]

Abstract

The article at hand contains exact asymptotic formulas for the distribution of conductors of elementary abelian p-extensions of global function fields of characteristic p. As a consequence for the distribution of discriminants, this leads to an exact asymptotic formula for simple cyclic extensions and an interesting lower bound for noncyclic elementary abelian extensions.

1. Main results

Let F be a global function field of characteristic p, that is a transcendental extension of degree 1 over some finite field $\mathbb{F}_q$ of cardinality q, and let $\mathbb{F}_q$ be algebraically closed in F. For an extension E/F, let $\mathfrak{f}(E/F)$ be its relative conductor, and $\|\mathfrak{f}(E/F)\| = q^{\deg \mathfrak{f}(E/F)}$ its absolute norm. The object of interest is the counting function

$$C(F, G; X) = |\{E/F : \operatorname{Gal}(E/F) \simeq G, \|\mathfrak{f}(E/F)\| \le X\}|$$

of field extensions E/F in a fixed algebraic closure of F with given finite Galois group G and bounded conductor. The values of this function coincides with finite coefficient sums of the Dirichlet series

$$\Phi(F, G; s) = \sum_{\operatorname{Gal}(E/F) \simeq G} \|\mathfrak{f}(E/F)\|^{-s},$$

generated by the extensions E/F with Galois group G. For the article at hand, we are interested in field extensions with elementary abelian Galois group of exponent p. These extensions are called Artin-Schreier extensions.

Theorem 1.1. *Let F be a global function field of characteristic p and $G = C_p^r$ be the elementary abelian group with exponent p and finite rank r. Let*

$$\alpha_p(G) = \frac{1 + (p-1)r}{p}$$

and

$$\beta(F, G) = \begin{cases} p-1 & r = 1 \\ 1 & r > 1. \end{cases}$$

Then the Dirichlet series $\Phi(F, G; s)$ has convergence abscissa $\alpha_p(G)$, and it possesses a meromorphic continuation, such that $\Phi(F, G; s) \prod_{l=2}^{p} \zeta_F(ls - (l-1)r)^{-1}$ is holomorphic for $\Re(s) > \alpha_p(G) - 1/(2p)$, where $\zeta_F(s)$ denotes the zeta function of F. The periodic pole $s = \alpha_p(G)$ with period $2\pi i / \log(q)$ has order $\beta(F, G)$, whereas the order of every other pole on the axis $\Re(s) = \alpha_p(G)$ does not exceed $\beta(F, G)$.

---

[*]Universität Paderborn, Institut für Mathematik, 33095 Paderborn, Germany. lagemann@math.uni-paderborn.de

The series $\Phi(F, G; s)$ is a power series in $t = q^{-s}$, which is convergent for $|t| < q^{-\alpha_p(G)}$, and its poles are located at $t = \xi q^{-\alpha_p(G)}$ for finitely many roots of unity ξ. If c_n denotes the n-th power series coefficient of $\Phi(F, G; s)$, we obtain $C(F, G; q^m) = \sum_{n=0}^{m} c_n$. By an application of the Cauchy integral formula, which is elaborated in Theorem Appendix A.5, this coefficient sum has the following asymptotic behaviour.

Theorem 1.2. *Let F be a global function field of characteristic p and $G = C_p^r$ be the elementary abelian group with exponent p and finite rank r. Then the number of Artin-Schreier extensions E/F with Galois group G has asymptotic*

$$C(F, G; X) \sim \gamma(F, G) \, X^{\alpha_p(G)} \, \log(X)^{\beta(F,G)-1}$$

with some explicitly computable constant $\gamma(F, G) > 0$.

The usage of asymptotic equivalence $f(X) \sim g(X)$ needs further comment. Usually this relation is defined by $\lim_{n \to \infty} f(n)/g(n) = 1$. Here, in the function field case that is, the counting functions $f(X)$ are step functions in $X = q^n$, where n runs over some arithmetic progression. Hence, the limit $\lim_{n \to \infty} f(n)/g(n)$ would not exist for continuous functions $g(X)$. Therefore, I write $f(X) \sim g(X)$ by abuse of notation, if there are integers $\ell \geq 1$, $e \geq 0$ with $\lim_{n \to \infty} f(q^{\ell n + e})/g(q^{\ell n + e}) = 1$. Analogously, I will make use of $f(X) \in \Omega(g(X))$ for $g(q^{\ell n + e}) \in O(f(q^{\ell n + e}))$, and $f(X) \in \Theta(g(X))$ for $f(q^{\ell n + e}) \in \Omega(g(q^{\ell n + e})) \cap O(g(q^{\ell n + e}))$. This redefinition is useful if one likes to compare function field asymptotics with number field asymptotics. Note that the constant $\gamma(F, G)$ in above theorem is not unique, varying by some q-powers, which depend on the chosen arithmetic progression. Disregarding this dichotomy, we obtain following formulas to compute $\gamma(F, G)$ for some arithmetic progression.

Addendum 1.3. *For $p = 2$ and $G = C_2^r$, we have*

$$\gamma(F, G) = \frac{|G|}{|\operatorname{Aut}(G)|} \frac{\log(q)}{1 - q^{-(r+1)}} \frac{\zeta_F(1)}{\zeta_F(r+1)}$$

where $\zeta_F(1)$ denotes the residue $\operatorname{Res}_{s=1}(\zeta_F(s))$.

Addendum 1.4. *For $p \neq 2$ and $G = C_p$, we have*

$$\gamma(F, G) = \frac{1}{(p-2)!} \frac{|G|}{|\operatorname{Aut}(G)|} \frac{\log(q)}{1 - q^{-1}} \frac{\zeta_F(1)^{p-1}}{p!} \prod_{\mathfrak{p}} \left(1 + (p-1) \|\mathfrak{p}\|^{-1}\right) \left(1 - \|\mathfrak{p}\|^{-1}\right)^{p-1}$$

where the product runs over the primes of F.

Formulas for $\gamma(F, C_p^r)$ with $p \neq 2$, $r \neq 1$ are within reach, but omitted, as they are less handy. Theorem 1.2 has also consequences on the distribution of discriminants $\mathfrak{d}(E/F)$ of Artin-Schreier extensions E/F, which shall be elaborated and be compared to other known results in the second section. Particularly Theorem 2.1 and Theorem 2.2 are very interesting with regard of the Malle conjecture, which is also introduced in the second section. After introducing some required notations and facts on class field theory, the proof of Theorem 1.1 starts with the fourth section, where the p-rank of ray class groups is computed. This leads to a nice local-global principle for Artin-Schreier extensions, and an explicit formula for the number $c_{\mathfrak{m}}$ of extensions with given conductor $\mathfrak{m}$ in the fifth section. In the sixth section then, we are able to give an explicit description of the analytic behaviour of the Dirichlet series $\Phi(F, G; s)$, which is generated by $c_{\mathfrak{m}}$. This leads to a proof of Theorem 1.1. In the last section, Theorem 1.2 and its addenda are proven, where it is the harder part to determine the constant $\gamma(F, G)$. Finally, the appendix contains a tauberian theorem for power series.

2. Consequences on the distribution of discriminants

For given global function field F and finite group G, consider the number of field extensions E/F in a fixed algebraic closure of F with Galois group G and bounded discriminant $\|\mathfrak{d}(E/F)\| = q^{\deg \mathfrak{d}(E/F)}$, that is the function

$$Z(F, G; X) = |\{E/F : \mathrm{Gal}(E/F) \simeq G, \|\mathfrak{d}(E/F)\| \leq X\}|.$$

For the elementary abelian group $G = C_p^r$, let

$$a_p(G) = \frac{\alpha_p(G)}{p^r - 1} = \frac{1 + (p-1)r}{p(p^r - 1)}.$$

Then we obtain the following theorems as corollaries of Theorem 1.2 and the Führerdiskriminantenformel.[1]

Theorem 2.1. *Let F be a global function field of characteristic p and $G = C_p$ be the simple cyclic group of order p. Then the number of Artin-Schreier extensions E/F with Galois group G has asymptotic*

$$Z(F, G; X) \sim c(F, G) \, X^{a_p(G)} \log(X)^{\beta(F,G)-1}$$

with $c(F, G) = \gamma(F, G)/(p-1)^{\beta(F,G)-1}$.

Proof. By the Führerdiskriminantenformel, a C_p-extension with conductor $\mathfrak{f}$ has discriminant $\mathfrak{d} = \mathfrak{f}^{p-1}$. We hence obtain the desired asymptotic formula from Theorem 1.2 and

$$Z(F, C_p; X) = C(F, C_p; X^{1/(p-1)}).$$

Note that the factor $1/(p-1)^{\beta(F,G)-1}$ of $c(F, G)$ originates from $\log(X^{1/(p-1)}) = \log(X)/(p-1)$. $\quad\square$

Theorem 2.2. *Let F be a global function field of characteristic p and $G = C_p^r$ be the elementary abelian group with exponent p and finite rank r. Then the number of Artin-Schreier extensions E/F with Galois group G has asymptotic*

$$Z(F, G; X) \in \Omega\left(X^{a_p(G)}\right).$$

Proof. By the Führerdiskriminantenformel, a C_p^r-extension with conductor $\mathfrak{f}$ has discriminant $\mathfrak{d} \mid \mathfrak{f}^m$ with $m = p^r - 1$, where equality corresponds to the case, in which every cyclic subextension has conductor $\mathfrak{f}$. We hence obtain

$$Z(F, C_p^r; X) \geq C(F, C_p^r; X^{1/m}) \in \Omega\left(X^{a_p(C_p^r)}\right),$$

by Theorem 1.2. $\quad\square$

In the same matter, we are able to give an upper bound for $Z(F, G; X)$, too. Therefore, let

$$d_p(G) = \frac{\alpha_p(G)}{p^r - p^{r-1}} = a_p(G) \frac{p^r - p^{r-1}}{p^r - 1}$$

for the elementary abelian group $G = C_p^r$.

Theorem 2.3. *Let F be a global function field of characteristic p and $G = C_p^r$ be the elementary abelian group with exponent p and finite rank r. Then the number of Artin-Schreier extensions E/F with Galois group G has asymptotic*

$$Z(F, G; X) \in O\left(X^{d_p(G)}\right).$$

---

[1]E.g. see formula (1.1) in [12].

Proof. Let E/F be a C_p^r-extension with conductor $\mathfrak{f}$ and discriminant $\mathfrak{d}$, and let $E_1, \ldots, E_r$ be a minimal set of cyclic subextensions with $E = E_1 \cdots E_r$. Since E/F has conductor $\mathfrak{f}$, one of the generating subfields has conductor $\mathfrak{f}$, too. Let E_1 be that field. By the Führerdiskriminantenformel, we now obtain $\mathfrak{f}^m \mid \mathfrak{d}$ with $m = p^r - p^{r-1}$, where equality corresponds to the case, in which $E_2, \ldots, E_r$ are unramified. Hence, every C_p^r-extension with discriminant norm X has conductor norm $X^{1/m}$ at most. This results in

$$Z(F, C_p^r; X) \leq C(F, C_p^r; X^{1/m}) \in \mathrm{O}\left(X^{d_p(C_p^r)}\right),$$

by Theorem 1.2. $\square$

As the number of extensions with given conductor grows at least linearly with its norm, it is more likely that all generating cyclic subextensions have the same conductor than that all but one are unramified. That means, the situation as considered for the lower bound happens far more often than the situation as considered for the upper bound. Hence, one might ask if $a_p(G)$ already gives the X-exponent of $Z(F, G; X)$. Lets now compare the results with the distribution of abelian groups in general. For the simple cyclic group, the formula of $c(F, C_p)$ gives a comparable function field result to the number field formula of Henri Cohen et al. [1], which is not completely analogous though. For abelian groups with order coprime to the characteristic, we obtain the following theorem by the results of David Wright [12]. His work only lacks a handy asymptotic formula for $Z(F, G; X)$ in the function field case, which we get by the redefinition of asymptotic equivalence as described in the beginning of this article.

Theorem (Wright [12]). *Let F be a global function or number field of characteristic $p \geq 0$ and G be a finite abelian group. Let ℓ be the smallest prime divisor of $|G|$, $G[\ell]$ the ℓ-torsion group of G, and $\tilde{F}$ the splitting field of $X^\ell - 1$ over F. Then we define*

$$a(G) = \frac{\ell}{|G|(\ell-1)}, \qquad b(F, G) = \frac{|G[\ell]| - 1}{[\tilde{F} : F]}.$$

Now assume $p \nmid |G|$. Then there is a positive constant $c(F, G)$, such that the number of G-extensions E/F has asymptotic

$$Z(F, G; X) \sim c(F, G)\, X^{a(G)}\, \log(X)^{b(F,G)-1}.$$

Proof. In the number field case, this is just Theorem I.2 loc. cit. In the function field case, this is the consequence of Theorem I.1 loc. cit., the discussion before Theorem I.3 loc. cit., and a tauberian theorem like Theorem Appendix A.5. $\square$

This result is restricted to the case $p \nmid |G|$. David Wright conjectured, that the case $p \mid |G|$ should behave analogously, but omitted the calculations as they are more involved. His formulas do indeed extend for the simple cyclic group C_p, and might also extend for the Klein four group C_2^2 in characteristic 2. But they do not hold for any other noncyclic elementary abelian group C_p^r, as the lower bound in Theorem 2.2 breaks the constant $a(G)$. This follows from the next proposition.

Proposition 2.4. *We have $a_p(C_p^r) = a(C_p^r)$ for $C_p^r = C_p, C_2^2$, and $a_p(C_p^r) > a(C_p^r)$ otherwise.*

Proof. Write $a_p(C_p^r) - a(C_p^r)$ as a fraction by extending $a_p(C_p^r)$ with the denominator of $a(C_p^r)$ and vice versa. Then this fraction has the numerator

$$\left((r-1)(p-1)^2 - p\right) \cdot p^{r-1} + p \geq 0,$$

which leads to the stated proposition. $\square$

This will have consequences on possible extensions of the Malle conjecture for global function fields.

EMC (Extended Malle Conjecture). *Let F be global field of characteristic $p \geq 0$ and G be a finite group. Then we conjecture, that there are positive constants $a(F,G)$, $b(F,G)$, $c(F,G)$, such that*

$$Z(F,G;X) \sim c(F,G)\, X^{a(F,G)} \, \log(X)^{b(F,G)-1}.$$

What are the formulas of these constants?

Gunter Malle [7, 8] proposed formulas for $a(F,G) = a(G)$ and $b(F,G)$ in the number field case, which extend Wright's formulas for abelian groups and other known results. While his conjecture for $b(F,G)$ needs some adjustments [6, 11], the formula for $a(F,G) = a(G)$, which remarkably does not depend on F, seems to be consistent for both number and function fields F with characteristic p coprime to the group order $|G|$. For function fields, this was shown by Jordan Ellenberg and Akshay Venkatesh [2] heuristically. With my results at hand, it is plausible that a general formula for $a(F,G)$ including the case $p \mid |G|$ is not independent of F and should at least depend on its characteristic p, a formula like $a(F,G) = a_p(G)$ for example. The main specialities of the case $p \mid |G|$ are, that every prime $\mathfrak{p}$ of F can wildly ramify in some G-extension E/F, and it is possible to have infinitely many local G-extensions $E/F_{\mathfrak{p}}$ over any localisation $F_{\mathfrak{p}}$. Both effects do not occur in the case $p \nmid |G|$, including number fields.

3. Notations and preliminaries

Let F denote a global function field with constant field $\mathbb{F}_q$ of cardinality q, algebraically closed in F. For a prime $\mathfrak{p}$ of F, let $\mathbb{F}_{\mathfrak{p}} \geq \mathbb{F}_q$ denote the residue class field, and $\|\mathfrak{p}\| = |\mathbb{F}_{\mathfrak{p}}|$ its norm. The valuation of $\mathfrak{p}$ is denoted by $v_{\mathfrak{p}}$. Let g_F be the genus, h_F the class number, and $\mathcal{Cl}$ the class group of F. In particular, we have $\mathcal{Cl} \simeq \mathbf{Z} \times \mathcal{Cl}[h_F]$. For a module $\mathfrak{m}$, an effective divisor of F that is, let $F^{\mathfrak{m}}$ be the multiplicative group of functions $x \in F^{\times}$ with divisor coprime to $\mathfrak{m}$, and let $F_{\mathfrak{m}} \leq F^{\mathfrak{m}}$ be the ray mod $\mathfrak{m}$ of functions $x \in F^{\mathfrak{m}}$ with $x \in 1 + \mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{m})}$ for all $\mathfrak{p} \mid \mathfrak{m}$. The ray class group $\mathcal{Cl}_{\mathfrak{m}}$ mod $\mathfrak{m}$ is defined by the exact sequence of abelian groups

$$1 \to \mathbb{F}_q^{\times} \to F^{\mathfrak{m}}/F_{\mathfrak{m}} \to \mathcal{Cl}_{\mathfrak{m}} \to \mathcal{Cl} \to 1. \tag{1}$$

By class field theory, there is a bijective map of finite abelian extensions E/F with module $\mathfrak{m}$ and subgroups $U \leq \mathcal{Cl}_{\mathfrak{m}}$ of finite index, such that $\mathrm{Gal}(E/F) \simeq \mathcal{Cl}_{\mathfrak{m}}/U$.[2] Let $U_{\mathfrak{m}}$ be the following finite p-group[3]

$$U_{\mathfrak{m}} = (F^{\mathfrak{m}}/F_{\mathfrak{m}})/(F^{\mathfrak{m}}/F_{\mathfrak{m}})^p \simeq \prod_{\mathfrak{p}^m || \mathfrak{m}} U_{\mathfrak{p}^m} \simeq \prod_{\mathfrak{p}^m || \mathfrak{m}} \langle 1 + \mathfrak{p} \rangle / \langle \langle 1 + \mathfrak{p}^m \rangle, \langle 1 + \mathfrak{p} \rangle^p \rangle, \tag{2}$$

where the product is to read as follows. The relation $\mathfrak{p}^m \,\|\, \mathfrak{m}$ stands for $v_{\mathfrak{p}}(\mathfrak{m}) = m > 0$. For an expression $f_{\mathfrak{p}}(m)$, the product $\prod_{\mathfrak{p}^m || \mathfrak{m}} f_{\mathfrak{p}}(m)$ stands for $\prod_{\mathfrak{p} | \mathfrak{m}} f_{\mathfrak{p}}(v_{\mathfrak{p}}(\mathfrak{m}))$. For example, let $f_{\mathfrak{p}}(m) = \mathfrak{p}^{m-1}$ and we have $\prod_{\mathfrak{p}^m || \mathfrak{m}} \mathfrak{p}^{m-1} = \prod_{\mathfrak{p} | \mathfrak{m}} \mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{m})-1}$, which is still an effective divisor. The same definition holds for sums. For example, the divisor above has degree $\sum_{\mathfrak{p}^m || \mathfrak{m}} (m-1) \deg \mathfrak{p} = \sum_{\mathfrak{p} | \mathfrak{m}} (v_{\mathfrak{p}}(\mathfrak{m}) - 1) \deg \mathfrak{p} \geq 0$. For the trivial module $\mathfrak{m} = \mathfrak{1}$, these products and sums are particularly defined as empty ones. Further, let $S = \{x \in F^{\times} : (x) = \mathfrak{a}^p \text{ for some divisor } \mathfrak{a}\}/F^p$ be the p-Selmer group, and let $S_{\mathfrak{m}} = \{[x] \in S : x \in F_{\mathfrak{m}}\}$ be the Selmer ray group mod $\mathfrak{m}$ of F.

---

[2] E.g. see page 139 and Theorem 9.23, page 140 in [9] for the sequence (1) and the Artin reciprocity law respectively.
[3] E.g. see section 9.2 in [4] for the isomorphisms.

4. Artin-Schreier extensions with given module

In this section, we shall compute the order of the ray class group $\mathcal{Cl}_{\mathfrak{m}}/\mathcal{Cl}_{\mathfrak{m}}^p$. It nearly behaves multiplicatively over the prime decomposition of $\mathfrak{m}$, if there were not the Selmer ray group $S_{\mathfrak{m}}$, whose order is not multiplicative. But as we will see, $S_{\mathfrak{m}}$ is trivial for almost all modules $\mathfrak{m}$ of interest. Proposition 4.1 is the function field analogue of Proposition 2.12 in [1], and its proof is essentially the same.

Proposition 4.1. *We have the exact sequence of finite abelian p-groups*

$$1 \to S_{\mathfrak{m}} \to \mathcal{Cl}[p] \to U_{\mathfrak{m}} \to \mathcal{Cl}_{\mathfrak{m}}/\mathcal{Cl}_{\mathfrak{m}}^p \to \mathcal{Cl}/\mathcal{Cl}^p \to 1.$$

Proof. The sequence (1) remains right exact by tensoring with C_p, and we obtain

$$U_{\mathfrak{m}} \to \mathcal{Cl}_{\mathfrak{m}}/\mathcal{Cl}_{\mathfrak{m}}^p \to \mathcal{Cl}/\mathcal{Cl}^p \to 1.$$

The kernel $U \leq U_{\mathfrak{m}}$ of the first map is generated by functions $x \in F^{\mathfrak{m}}$ with divisor $(x) = (y)\,\mathfrak{a}^p$ and $y \in F_{\mathfrak{m}}$. Therefore, any class $[x] = [xy^{-1}]$ in U is generated by a Selmer element $[z] \in S$ with $(z) = \mathfrak{a}^p$. Conversely, every Selmer class $[x] \in S$ can be mapped in U by the approximation theorem,[4] and this map has kernel $S_{\mathfrak{m}}$. Finally, we use the following isomorphism of the p-torsion group $\mathcal{Cl}[p]$ with the Selmer group S. For a given divisor class $[\mathfrak{a}] \in \mathcal{Cl}[p]$, there is a function $z \in F^{\times}$ with divisor $(z) = \mathfrak{a}^p$, and vice versa. Then the map $[\mathfrak{a}] \mapsto [z]$ is well defined and provides an isomorphism $\mathcal{Cl}[p] \simeq S$. $\square$

Lemma 4.2. *For any integer $m \geq 1$, let $r_m = m - 1 - \lfloor (m-1)/p \rfloor$, and $r_0 = 0$. Let $\mathfrak{m}$ be a module. Then we have*

$$(\mathcal{Cl}_{\mathfrak{m}} : \mathcal{Cl}_{\mathfrak{m}}^p) = p\,|S_{\mathfrak{m}}||U_{\mathfrak{m}}| = p\,|S_{\mathfrak{m}}| \prod_{\mathfrak{p}^m||\mathfrak{m}} \|\mathfrak{p}\|^{r_m}.$$

Proof. With the exact sequence of Proposition 4.1 and the isomorphism in (2), we obtain

$$(\mathcal{Cl}_{\mathfrak{m}} : \mathcal{Cl}_{\mathfrak{m}}^p) = \frac{|S_{\mathfrak{m}}||U_{\mathfrak{m}}|\,(\mathcal{Cl} : \mathcal{Cl}^p)}{|\mathcal{Cl}[p]|} = p\,|S_{\mathfrak{m}}|\,|U_{\mathfrak{m}}| = p\,|S_{\mathfrak{m}}| \prod_{\mathfrak{p}^m||\mathfrak{m}} |U_{\mathfrak{p}^m}|.$$

By the well-known Einseinheitensatz,[5] the p-rank of $U_{\mathfrak{p}^m}$ is $[\mathbb{F}_{\mathfrak{p}} : \mathbb{F}_p]\,r_m$, and we obtain the proposed index formula. $\square$

Corollary 4.3. *Let $\mathfrak{m} = \mathfrak{n}\mathfrak{p}$ be a module with prime divisor $\mathfrak{p}$ coprime to $\mathfrak{n}$. Then $|S_{\mathfrak{m}}| = |S_{\mathfrak{n}}|$ holds.*

Proof. Any ramified p-extension of the local field $F_{\mathfrak{p}}$ is wildly ramified, whence its local conductor cannot be squarefree. This implies that an abelian p-extension of F with module $\mathfrak{m}$ cannot be ramified in $\mathfrak{p}$, and abelian p-extensions of F with conductor $\mathfrak{m}$ are nonexistent. Hence, the ray class factor groups $\mathcal{Cl}_{\mathfrak{m}}/\mathcal{Cl}_{\mathfrak{m}}^p$ and $\mathcal{Cl}_{\mathfrak{n}}/\mathcal{Cl}_{\mathfrak{n}}^p$ are isomorphic, and the proposed coincidence of cardinality follows from Lemma 4.2 and $|U_{\mathfrak{p}}| = 1$. $\square$

The order of Selmer ray groups is hard to compute in general. For modules with a large square divisor however, we can utilise the embedding of the Selmer group in the group of regular logarithmic differentials of F.

---

[4]E.g. see Theorem 1.3.1, page 12 in [10].
[5]E.g. see Proposition 6.2, page 18 in [3].

Lemma 4.4. *Let* $\mathfrak{m}$ *be a module with the condition*

$$\sum_{\mathfrak{p}^m || \mathfrak{m}} (m-1) \deg \mathfrak{p} > 2g_F - 2.$$

Then the Selmer ray group $S_\mathfrak{m}$ is trivial.

Proof. Let Ω_F be the group of differentials and

$$\psi : S_\mathfrak{m} \to \Omega_F, \quad [x] \mapsto \frac{dx}{x}.$$

By the product rule, this map is well defined and homomorphic via

$$\frac{d(xy)}{xy} = \frac{ydx + xdy}{xy} = \frac{dx}{x} + \frac{dy}{y} \qquad \text{and} \qquad \frac{dz^p}{z^p} = p \cdot \frac{dz}{z} = 0$$

for $x, y, z \in F^\times$. The differential dx is zero if and only if $x = z^p$ is a nonseparating element of F.[6] Therefore, ψ is injective. We now suppose $x \in F_\mathfrak{m}$ to generate a nontrivial Selmer class in $S_\mathfrak{m}$, and denote its logarithmic differential with $\omega = dx/x$. For any prime $\mathfrak{p}$ of F with uniformizing element t, there is an integer $i = -v_\mathfrak{p}(x)/p$, such that $u = xt^{ip}$ is a unit modulo $\mathfrak{p}$. We hence obtain $\omega = du/u$ by the product rule, and $\omega = (du/dt)(dt/u)$ by the chain rule. This yields

$$v_\mathfrak{p}(\omega) = v_\mathfrak{p}(du/dt) - v_\mathfrak{p}(u) + v_\mathfrak{p}(dt) = v_\mathfrak{p}(du/dt).$$

Observe, that $v_\mathfrak{p}(dt) = 0$ follows from $v_\mathfrak{p}(t) = 1$.[7] The series expansion of $u = \sum a_n t^n$ with respect to t contains at least one nontrivial term $a_n t^n$ with $p \nmid n$, as u is no p-th power. If n is chosen to be minimal with this property, we have $n \geq 1$ and $du/dt \in na_n t^{n-1}\langle 1 + \mathfrak{p} \rangle$, whence ω has positive valuation $v_\mathfrak{p}(\omega) = n - 1$. As we have chosen $\mathfrak{p}$ to be arbitrary, ω is hence regular, and has a positive divisor of degree $2g_F - 2$.[8] This already leads to a contradiction in case of $g_F = 0$, of course, but more generally, we yield the inequality

$$2g_F - 2 = \deg(\omega) \geq \sum_{\mathfrak{p} | \mathfrak{m}} v_\mathfrak{p}(\omega) \deg \mathfrak{p}.$$

Since x is chosen from the ray $F_\mathfrak{m}$, we have $x \in \langle 1 + \mathfrak{p}^m \rangle$ for $\mathfrak{p}^m \, || \, \mathfrak{m}$. Then the integer n, obtained by the procedure above, fulfils $n \geq m$, which implies $v_\mathfrak{p}(\omega) \geq m - 1$ and

$$2g_F - 2 \geq \sum_{\mathfrak{p}^m || \mathfrak{m}} (m-1) \deg \mathfrak{p}.$$

Since $\mathfrak{m}$ is a module violating this inequality, we yield the desired contradiction to the existence of x. Hence, the Selmer ray group $S_\mathfrak{m}$ only contains the trivial class. $\square$

5. Artin-Schreier extensions with given conductor

With the results of the last section, we easily obtain the number of Artin-Schreier extensions with given module. If we like to count extensions with given conductor, we are led to an inclusion-exclusion principle via the Möbius formula.

---

[6]E.g. see Proposition 3.10.2 (d), page 144, and Proposition 4.1.8 (c), page 160 in [10].
[7]E.g. see Theorem 4.3.2 (e), page 171 in [10].
[8]E.g. see Corollary 1.5.16, page 31 in [10].

Proposition 5.1. *For any module $\mathfrak{m}$, let $c_{\mathfrak{m}}$ be the number of C_p^r-extensions E/F with conductor $\mathfrak{m}$. Further, let*

$$e(X) = \prod_{i=0}^{r-1} \frac{pX - p^i}{p^r - p^i} = \sum_{i=0}^{r} e_i X^i.$$

Then we have $c_{\mathbf{1}} = e(|\mathcal{Cl}[p]|)$ for the trivial module $\mathfrak{m} = \mathbf{1}$, and

$$c_{\mathfrak{m}} = \sum_{i=1}^{r} e_i \sum_{\mathfrak{n}|\mathfrak{m}} \mu(\mathfrak{m}\mathfrak{n}^{-1}) |S_{\mathfrak{n}}|^i |U_{\mathfrak{n}}|^i$$

for nontrivial modules $\mathfrak{m} \neq \mathbf{1}$, where $\mu(\mathfrak{n})$ denotes the Möbius function for modules.

Proof. For any elementary abelian group A, the number of subgroups $U \leq A$ with factor group $A/U \simeq C_p^r$ is given by $e(|A|/p)$.[9] Note that we do not need any assumptions on the p-rank of A, since $e(p^i) = 0$ hold for $0 \leq i \leq r - 2$. Hence, by Lemma 4.2, the number of all C_p^r-extensions E/F with module $\mathfrak{m}$ sums up to

$$e(|S_{\mathfrak{m}}||U_{\mathfrak{m}}|) = \sum_{\mathfrak{n}|\mathfrak{m}} c_{\mathfrak{n}}.$$

Now, $c_{\mathbf{1}} = e(|\mathcal{Cl}[p]|)$ follows for the trivial module $\mathfrak{m} = \mathbf{1}$, since we have $S_{\mathbf{1}} = S \simeq \mathcal{Cl}[p]$ and $U_{\mathbf{1}} = 1$. Further, we obtain

$$c_{\mathfrak{m}} = \sum_{\mathfrak{n}|\mathfrak{m}} \mu(\mathfrak{m}\mathfrak{n}^{-1}) e(|S_{\mathfrak{n}}||U_{\mathfrak{n}}|) = \sum_{i=0}^{r} e_i \sum_{\mathfrak{n}|\mathfrak{m}} \mu(\mathfrak{m}\mathfrak{n}^{-1}) |S_{\mathfrak{n}}|^i |U_{\mathfrak{n}}|^i$$

by the inversion formula of Möbius. The sum $\sum_{\mathfrak{n}|\mathfrak{m}} \mu(\mathfrak{n})$ vanishes for nontrivial modules $\mathfrak{m} \neq \mathbf{1}$, whence the formula for $c_{\mathfrak{m}}$ only depends on the indices $i = 1, \ldots, r$. $\qquad\square$

With the Möbius formula for $c_{\mathfrak{m}}$, we near a local-global principle for the number of Artin-Schreier extensions. For example, suppose that the Selmer group S of F was trivial. Then all Selmer ray groups are trivial, and we would obtain

$$c_{\mathfrak{m}} = \sum_{i=1}^{r} e_i \sum_{\mathfrak{n}|\mathfrak{m}} \mu(\mathfrak{m}\mathfrak{n}^{-1}) |U_n|^i = \sum_{i=1}^{r} e_i \prod_{\mathfrak{p}^m || \mathfrak{m}} \left(|U_{\mathfrak{p}^m}|^i - |U_{\mathfrak{p}^{m-1}}|^i \right).$$

The second equation, which we later shall prove in detail, is just a consequence of the multiplicativity of $\mu(\mathfrak{n})$ and $|U_{\mathfrak{n}}|^i$. By Lemma 4.4, we might hope for formulas like the above, since the Selmer ray group $S_{\mathfrak{m}}$ is trivial for modules $\mathfrak{m}$ with a large square divisor. But we must carefully regard the Selmer ray groups $S_{\mathfrak{n}}$ for divisors $\mathfrak{n} \mid \mathfrak{m}$, too. With the following lemma, we shall see, that a huge family of modules allows above formula, whereas formulas for the infinite complementary family depends only on finitely many modules. This yields a crucial tool for computing $\Phi(F, C_p^r; s)$ in the next section. Call a module $\mathfrak{m}$ squareful, if every prime divisor $\mathfrak{p} \mid \mathfrak{m}$ has at least order $v_{\mathfrak{p}}(\mathfrak{m}) \geq 2$. Let $\mathcal{M}$ be the finite set consisting of the trivial module $\mathfrak{m} = \mathbf{1}$ and the squareful modules $\mathfrak{m}$ supported only by primes $\mathfrak{p}$ with $\deg \mathfrak{p} \leq 2g_F - 2$ and $v_{\mathfrak{p}}(\mathfrak{m}) \leq 2g_F$. Note that $\mathcal{M}$ consists only of the trivial module in case of $g_F = 0, 1$.

Lemma 5.2. *The number $c_{\mathfrak{m}}$ of C_p^r-extensions E/F with conductor $\mathfrak{m}$ fulfils the following formulas.*

(a) *Let $\mathfrak{m} = \mathbf{1}$ be the trivial module. Then $c_{\mathbf{1}} = e(|\mathcal{Cl}[p]|)$ holds.*

---

[9]E.g. see Hilfssatz 8.5, page 311 in [5].

(b) *Let* $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_1^2$ *with* $\mathfrak{m}_0 \in \mathcal{M}$ *and* $\mathfrak{m}_1$ *being a squarefree module supported by primes* $\mathfrak{p}$ *of degree* $\deg\mathfrak{p} > 2g_F - 2$ *only. Then*

$$c_{\mathfrak{m}} = \mu(\mathfrak{m}_1)\tilde{c}_{\mathfrak{m}_0} + \sum_{i=1}^{r} e_i \prod_{\mathfrak{p}^m||\mathfrak{m}} \left(\|\mathfrak{p}\|^{ir_m} - \|\mathfrak{p}\|^{ir_{m-1}} \right)$$

holds with $\tilde{c}_{\mathbf{1}} = c_{\mathbf{1}} - \sum_{i=0}^{r} e_i$ *for the trivial module* $\mathfrak{m}_0 = \mathbf{1}$ *and*

$$\tilde{c}_{\mathfrak{m}_0} = c_{\mathfrak{m}_0} - \sum_{i=1}^{r} e_i \prod_{\mathfrak{p}^m||\mathfrak{m}_0} \left(\|\mathfrak{p}\|^{ir_m} - \|\mathfrak{p}\|^{ir_{m-1}} \right)$$

otherwise.

(c) *Let* $\mathfrak{m}$ *be a module not covered by* (a,b). *Then*

$$c_{\mathfrak{m}} = \sum_{i=1}^{r} e_i \prod_{\mathfrak{p}^m||\mathfrak{m}} \left(\|\mathfrak{p}\|^{ir_m} - \|\mathfrak{p}\|^{ir_{m-1}} \right)$$

holds. In particular, we have $c_{\mathfrak{m}} = 0$ *if* $\mathfrak{m}$ *is not squareful, or more generally, has a prime divisor* $\mathfrak{p}$ *with valuation* $v_{\mathfrak{p}}(\mathfrak{m}) \equiv 1 \pmod{p}$.

Note that this lemma does not provide any information on $c_{\mathfrak{m}}$ for $\mathfrak{m} \in \mathcal{M} \setminus \{\mathbf{1}\}$.

Proof. Assertion (a) is just a restatement of Proposition 5.1. For the rest of the proof, we can consider $\mathfrak{m}$ to be nontrivial. Let $a_{\mathfrak{m}}$ be given by $a_{\mathfrak{m}} = c_{\mathfrak{m}} - b_{\mathfrak{m}}$ and

$$b_{\mathfrak{m}} = \sum_{i=1}^{r} e_i \prod_{\mathfrak{p}^m||\mathfrak{m}} \left(\|\mathfrak{p}\|^{ir_m} - \|\mathfrak{p}\|^{ir_{m-1}} \right).$$

Then assertions (b) and (c) are equivalent to $a_{\mathfrak{m}} = \mu(\mathfrak{m}_1)\tilde{c}_{\mathfrak{m}_0}$ and $a_{\mathfrak{m}} = 0$ respectively. Note that $\tilde{c}_{\mathbf{1}} = a_{\mathbf{1}} - e_0$ and $\tilde{c}_{\mathfrak{m}_0} = a_{\mathfrak{m}_0}$ hold for $\mathfrak{m}_0 \neq \mathbf{1}$. We start with the identity $\|\mathfrak{p}\|^{ir_m} = |U_{\mathfrak{p}^m}|^i$ provided by Lemma 4.2. Then

$$\|\mathfrak{p}\|^{ir_m} - \|\mathfrak{p}\|^{ir_{m-1}} = |U_{\mathfrak{p}^m}|^i - |U_{\mathfrak{p}^{m-1}}|^i = \sum_{n=0}^{m} \mu(\mathfrak{p}^{m-n})|U_{\mathfrak{p}^n}|^i$$

follows, as $\mu(\mathfrak{n})$ vanishes on squares. The order $|U_{\mathfrak{n}}|^i$ provides a multiplicative function for modules, whence we obtain

$$\prod_{\mathfrak{p}^m||\mathfrak{m}} \sum_{n=0}^{m} \mu(\mathfrak{p}^{m-n})|U_{\mathfrak{p}^n}|^i = \sum_{\mathfrak{n}|\mathfrak{m}} \mu(\mathfrak{m}\mathfrak{n}^{-1}) \prod_{\mathfrak{p}^n||\mathfrak{n}} |U_{\mathfrak{p}^n}|^i = \sum_{\mathfrak{n}|\mathfrak{m}} \mu(\mathfrak{m}\mathfrak{n}^{-1})|U_{\mathfrak{n}}|^i.$$

Putting all together, this results in

$$b_{\mathfrak{m}} = \sum_{i=1}^{r} e_i \sum_{\mathfrak{n}|\mathfrak{m}} \mu(\mathfrak{m}\mathfrak{n}^{-1})|U_{\mathfrak{n}}|^i. \tag{3}$$

As we consider $\mathfrak{m}$ to be nontrivial, we obtain

$$a_{\mathfrak{m}} = c_{\mathfrak{m}} - b_{\mathfrak{m}} = \sum_{i=1}^{r} e_i \sum_{\mathfrak{n}|\mathfrak{m}} \mu(\mathfrak{m}\mathfrak{n}^{-1})(|S_{\mathfrak{n}}|^i - 1)|U_{\mathfrak{n}}|^i \tag{4}$$

by Proposition 5.1. Now, let $\mathfrak{m}$ be a module as considered in assertion (c). Then there is a multiple prime divisor $\mathfrak{p}^m \parallel \mathfrak{m}$ with $m > 2$, such that $\deg\mathfrak{p} > 2g_F - 2$ or $m > 2g_F$ holds. Any divisor $\mathfrak{n} \mid \mathfrak{m}$ with

9

$\mu(\mathfrak{m}\mathfrak{n}^{-1}) \neq 0$ is divisible by $\mathfrak{p}^{m-1}$, whence its Selmer ray group $S_\mathfrak{n}$ is trivial by Lemma 4.4. This yields $a_\mathfrak{m} = 0$ by formula (4), as desired. Now, let $\mathfrak{m} = \mathfrak{m}_0 \mathfrak{m}_1^2$ be a module as considered in assertion (b). Any divisor $\mathfrak{n} \mid \mathfrak{m}$ with $\mu(\mathfrak{m}\mathfrak{n}^{-1}) \neq 0$ has necessarily the form $\mathfrak{n} = \mathfrak{n}_0 \mathfrak{m}_1 \mathfrak{n}_1$ with $\mathfrak{n}_0 \mid \mathfrak{m}_0$ and $\mathfrak{n}_1 \mid \mathfrak{m}_1$, as $\mathfrak{m}\mathfrak{n}^{-1}$ would contain a square otherwise. Considering this form of $\mathfrak{n}$, the Selmer ray group $S_\mathfrak{n}$ is trivial for $\mathfrak{n}_1 \neq \mathfrak{1}$ by Lemma 4.4. Hence, the right hand side in formula (4) only depends on modules $\mathfrak{n} = \mathfrak{n}_0 \mathfrak{m}_1$ with $\mathfrak{n}_0 \mid \mathfrak{m}_0$, and we are led to

$$a_\mathfrak{m} = \sum_{i=1}^r e_i \sum_{\mathfrak{n}_0 \mid \mathfrak{m}_0} \mu(\mathfrak{m}\mathfrak{n}_0^{-1}\mathfrak{m}_1^{-1})(|S_{\mathfrak{n}_0\mathfrak{m}_1}|^i - 1)|U_{\mathfrak{n}_0\mathfrak{m}_1}|^i$$

Since $\mathfrak{m}_1$ is squarefree, we have $|U_{\mathfrak{m}_1}| = 1$ and $|S_{\mathfrak{n}_0\mathfrak{m}_1}| = |S_{\mathfrak{n}_0}|$ by Lemma 4.2 and Corollary 4.3 respectively. Using the multiplicativity of $\mu(\mathfrak{n})$ and $|U_\mathfrak{n}|$, we now obtain

$$a_\mathfrak{m} = \mu(\mathfrak{m}_1) \sum_{i=1}^r e_i \sum_{\mathfrak{n}_0 \mid \mathfrak{m}_0} \mu(\mathfrak{m}_0\mathfrak{n}_0^{-1})(|S_{\mathfrak{n}_0}|^i - 1)|U_{\mathfrak{n}_0}|^i.$$

With the formula for $a_{\mathfrak{m}_0}$ given by formula (4), this implies the desired identity $a_\mathfrak{m} = \mu(\mathfrak{m}_1)\tilde{c}_{\mathfrak{m}_0}$ in the case $\mathfrak{m}_0 \neq \mathfrak{1}$. If $\mathfrak{m}_0 = \mathfrak{1}$ is the trivial module, we obtain

$$a_\mathfrak{m} = \mu(\mathfrak{m}_1) \sum_{i=1}^r e_i(|S|^i - 1) = \mu(\mathfrak{m}_1)\left(e(|S|) - e_0 - \sum_{i=1}^r e_i\right) = \mu(\mathfrak{m}_1)\tilde{c}_\mathfrak{1}$$

as a consequence of assertion (a). $\qquad\square$

6. Dirichlet series of Artin-Schreier extensions

This section contains a rather complete description of the Dirichlet series

$$\Phi(F, C_p^r; s) = \sum_{\mathrm{Gal}(E/F) \simeq C_p^r} \|\mathfrak{f}(E/F)\|^{-s} = \sum_\mathfrak{m} c_\mathfrak{m}\|\mathfrak{m}\|^{-s},$$

generated by the C_p^r-extensions E/F and by the modules $\mathfrak{m}$ of F respectively. As a consequence of Lemma 5.2, the series $\Phi(F, C_p^r; s)$ can be decomposed in a finite sum of Euler products $\Phi_i(s)$ and an error term $\Upsilon_r(s)$ with

$$\Phi_i(s) = \prod_\mathfrak{p} \left(1 + (\|\mathfrak{p}\|^i - 1)\sum_{p\nmid n} \|\mathfrak{p}\|^{ir_n - (n+1)s}\right). \tag{5}$$

Lemma 6.1. *The Dirichlet series $\Phi(F, C_p^r; s)$ has the decomposition*

$$\Phi(F, C_p^r; s) = \sum_{i=1}^r e_i \Phi_i(s) + \Upsilon_r(s),$$

where $\Upsilon_r(s)$ is a rational function in $t = q^{-s}$ without poles for $\Re(s) > 1/4$.

Proof. Let $\Phi_{i,\mathfrak{p}}(s)$ be the Euler factor of $\Phi_i(s)$ corresponding to the prime $\mathfrak{p}$. By definition in Lemma 4.2, we have $r_n = n - 1 - \lfloor (n-1)/p \rfloor$. Since $r_{n+1} = r_n$ holds for $p \mid n$, and $r_{n+1} = 1 + r_n$ otherwise, it is easy to verify

$$\Phi_{i,\mathfrak{p}}(s) = 1 + (\|\mathfrak{p}\|^i - 1)\sum_{p\nmid n} \|\mathfrak{p}\|^{ir_n - (n+1)s} = 1 + \sum_{m\geq 1}(\|\mathfrak{p}\|^{ir_m} - \|\mathfrak{p}\|^{ir_{m-1}})\|\mathfrak{p}\|^{-ms}$$

by the transformation $m = n + 1$. We hence obtain

$$\sum_{i=1}^{r} e_i \Phi_i(s) = \sum_{\mathfrak{m}} \left(\sum_{i=1}^{r} e_i \prod_{\mathfrak{p}^m || \mathfrak{m}} \left(\|\mathfrak{p}\|^{irm} - \|\mathfrak{p}\|^{irm-1} \right) \right) \|\mathfrak{m}\|^{-s}.$$

The coefficient of the latter Dirichlet series corresponding to $\mathfrak{m}$ coincides with $c_\mathfrak{m}$, if $\mathfrak{m}$ is of the form as considered in Lemma 5.2 (c). Therefore, the difference $\Upsilon_r(s) = \Phi(F, C_p^r; s) - \sum_{i=1}^{r} e_i \Phi_i(s)$ is generated by the modules $\mathfrak{m}$ as considered in Lemma 5.2 (a,b). Then we obtain

$$\Upsilon_r(s) = \left(c_\mathfrak{1} - \sum_{i=1}^{r} e_i \right) + \left(\sum_{\mathfrak{m}_0 \in \mathcal{M}} \tilde{c}_{\mathfrak{m}_0} \|\mathfrak{m}_0\|^{-s} \prod_{\deg \mathfrak{p} > 2g_F - 2} (1 - \|\mathfrak{p}\|^{-2s}) \right),$$

where the big parentheses correspond to case (a) and (b) respectively. Note hereby, that the restricted Euler product $\prod(1 - \|\mathfrak{p}\|^{-2s})$ equals the restricted series $\sum \mu(\mathfrak{m}_1)\|\mathfrak{m}_1\|^{-2s}$ generated by the modules $\mathfrak{m}_1$ as given in (b). Since $\mathcal{M}$ is finite, the sum over its elements is a polynomial $f(q^{-s})$ in q^{-s}. Furthermore, there are only finitely many primes $\mathfrak{p}$ of degree $\deg \mathfrak{p} \leq 2g_F - 2$, and the product $g(q^{-s})$ over their Euler factors $(1 - \|\mathfrak{p}\|^{-2s})$ is a polynomial as well. Consequently, $\Upsilon_r(s)$ is rational in q^{-s} with formula

$$\Upsilon_r(s) = c_\mathfrak{1} - \sum_{i=1}^{r} e_i + \frac{f(q^{-s})}{g(q^{-s})} \zeta_F(2s)^{-1}, \tag{6}$$

where $\zeta_F(s)$ is the zeta function of F. The poles of $\Upsilon_r(s)$ are located on the imaginary axes $\Re(s) = 0$, corresponding to the zeros of $g(q^{-s})$, and $\Re(s) = 1/4$, corresponding to the zeros of $\zeta_F(2s)$ by the theorem of Hasse-Weil, also known as the function field analogue of the Riemann hypothesis.[10] $\qquad \square$

Note that we could compute the function $\Upsilon_r(s)$ with formula (6) and the knowledge of only finitely many values of $c_\mathfrak{m}$, namely those for $\mathfrak{m} \in \mathcal{M}$. Hence, the infinite set of modules, which values of $c_\mathfrak{m}$ do not behave uniformly, yield a quite manageable error term, but it depends strongly on the given field F. The dependence on $G = C_p^r$ is very loosely. For the Euler products $\Phi_i(s)$ however, there is virtually no dependence on F and G, only it is defined over the primes of F, and $i \leq r$ holds, of course. We hence can investigate the Euler product $\Phi_r(s)$ in its own right for any integer $r \geq 1$, and aim to describe $\Phi_r(s)$ as a product of zeta functions.

Proposition 6.2. *The Euler factors $\Phi_{r,\mathfrak{p}}(s)$ of $\Phi_r(s)$ are meromorphic continuable for all complex arguments s with*

$$\Phi_{r,\mathfrak{p}}(s) = \left(1 - \|\mathfrak{p}\|^{-s}\|\mathfrak{p}\|^{(p-1)(r-s)} \right)^{-1} \left(1 + \|\mathfrak{p}\|^{-s} \sum_{l=0}^{p-2} \|\mathfrak{p}\|^{l(r-s)} \right) \left(1 - \|\mathfrak{p}\|^{-s} \right).$$

Proof. Consider the sum running over $p \nmid n$ of the Euler factor $\Phi_{r,\mathfrak{p}}(s)$ as given in (5). The occurring $\|\mathfrak{p}\|$-exponents are of the form $rr_n - (n+1)s$. By definition in Lemma 4.2, we have $r_n = n - 1 - \lfloor (n-1)/p \rfloor$. As n is indivisible by p, we can write $n = kp + l + 1$ for some $k \geq 0$ and $0 \leq l \leq p - 2$, and $r_n = k(p-1) + l$ follows. Altogether, we obtain

$$rr_n - (n+1)s = k((p-1)r - ps) + l(r-s) - 2s$$

---

and

$$\sum_{\mathfrak{p} \nmid n} \|\mathfrak{p}\|^{rr_n - (n+1)s} = \sum_{k \geq 0} \sum_{l=0}^{p-2} \|\mathfrak{p}\|^{k((p-1)r - ps)} \|\mathfrak{p}\|^{l(r-s)} \|\mathfrak{p}\|^{-2s}.$$

This series is convergent for $\Re(s) > (p-1)r/p$, and meromorphic continuable beyond its abscissa via the rational function

$$\left(1 - \|\mathfrak{p}\|^{(p-1)r - ps}\right)^{-1} \sum_{l=0}^{p-2} \|\mathfrak{p}\|^{l(r-s)} \|\mathfrak{p}\|^{-2s}.$$

The same holds for the Euler factor $\Phi_{r,\mathfrak{p}}(s)$, and its meromorphic continuation has the form

$$\Phi_{r,\mathfrak{p}}(s) = \left(1 - \|\mathfrak{p}\|^{(p-1)r - ps}\right)^{-1} \left(1 - \|\mathfrak{p}\|^{(p-1)r - ps} + (\|\mathfrak{p}\|^r - 1) \sum_{l=0}^{p-2} \|\mathfrak{p}\|^{l(r-s)} \|\mathfrak{p}\|^{-2s}\right).$$

We hence have verified one proposed factor of $\Phi_{r,\mathfrak{p}}(s)$. Further, the latest term of the right hand side has the identity

$$(\|\mathfrak{p}\|^r - 1) \sum_{l=0}^{p-2} \|\mathfrak{p}\|^{l(r-s)} \|\mathfrak{p}\|^{-2s} = \sum_{l=1}^{p-1} \|\mathfrak{p}\|^{lr - (l+1)s} - \sum_{l=0}^{p-2} \|\mathfrak{p}\|^{lr - (l+2)s}$$

$$= \|\mathfrak{p}\|^{(p-1)r - ps} - \|\mathfrak{p}\|^{-2s} + \sum_{l=1}^{p-2} \|\mathfrak{p}\|^{lr - (l+1)s} (1 - \|\mathfrak{p}\|^{-s}).$$

Now, extend the latest sum with the index $l = 0$ and subtract the corresponding term $\|\mathfrak{p}\|^{-s} - \|\mathfrak{p}\|^{-2s}$ to obtain the factorisation of $\Phi_{r,\mathfrak{p}}(s)$ as stated. $\square$

Lemma 6.3. *The Dirichlet series $\Phi_r(s)$ has the meromorphic continuation $\Phi_r(s) = \Psi_r(s)\Lambda_r(s)$ for $\Re(s) > \alpha_p(C_p^r) - \varepsilon$ and some $\varepsilon > 1/(2p)$ with meromorphic factor*

$$\Lambda_r(s) = \prod_{l=2}^{p} \zeta_F(ls - (l-1)r)$$

and holomorphic factor

$$\Psi_r(s) = \prod_{\mathfrak{p}} \left(1 + \|\mathfrak{p}\|^{-s} \sum_{l=0}^{p-2} \|\mathfrak{p}\|^{l(r-s)}\right) \prod_{l=0}^{p-2} \left(1 - \|\mathfrak{p}\|^{-s} \|\mathfrak{p}\|^{l(r-s)}\right).$$

Proof. Let $\mathfrak{p}$ be an arbitrary prime of F. Then the Euler factor $\Psi_{r,\mathfrak{p}}(s)$ is an entire function, and by Proposition 6.2, we yield the identity of meromorphic functions

$$\Phi_{r,\mathfrak{p}}(s) \Psi_{r,\mathfrak{p}}(s)^{-1} = \left(1 - \|\mathfrak{p}\|^{(p-1)(r-s)-s}\right)^{-1} \prod_{l=1}^{p-2} \left(1 - \|\mathfrak{p}\|^{l(r-s)-s}\right)^{-1} = \Lambda_{r,\mathfrak{p}}(s).$$

Observe the substitution $l+1$ for l to get the latter equality. Hence, the Euler factors of $\Phi_r(s)$ and $\Lambda_r(s)\Psi_r(s)$ coincide for all complex arguments s. Thus a meromorphic continuation of $\Phi_r(s)$ is given by $\Lambda_r(s)\Psi_r(s)$ for at least in the region of convergence of $\Psi_r(s)$, which is left to be determined. Note the fact on infinite products, that $\prod(1+a_n)$ is absolutely convergent if and only if $\sum a_n$ is absolutely convergent. Furthermore, $\sum \|\mathfrak{p}\|^{-s}$ is absolutely convergent for $\Re(s) > 1$ only. Since the Euler factors of $\Psi_r(s)$ are finite sums of length not depending on the corresponding prime $\mathfrak{p}$, it is sufficient to show, that all $\|\mathfrak{p}\|$-exponents of $\Psi_{r,\mathfrak{p}}(s)$ are

less than -1 for real arguments $s > \alpha_p(C_p^r) - \varepsilon$ and some $\varepsilon > 1/(2p)$. There are integers $a(l_1, \ldots, l_k)$, not depending on $\mathfrak{p}$ and zero for almost all $k \geq 1$, such that

$$\Psi_{r,\mathfrak{p}}(s) = 1 + \sum_{k \geq 1} \|\mathfrak{p}\|^{-ks} \sum_{0 \leq l_1, \ldots, l_k \leq p-2} a(l_1, \ldots, l_k) \, \|\mathfrak{p}\|^{(l_1 + \ldots + l_k)(r-s)}.$$

It is easy to see that $a(l) = 0$ holds for $0 \leq l \leq p - 2$. Furthermore, $a(l_1, \ldots, l_k) = 0$ holds for $k > p$. Hence, the $\|\mathfrak{p}\|$-exponents of interest have the form $-ks + (l_1 + \ldots + l_k)(r - s)$ with $2 \leq k \leq p$ and $0 \leq l_1, \ldots, l_k \leq p-2$. They are less than -1 for $s > (1 + (l_1 + \ldots + l_k)r)/(k + l_1 + \ldots + l_k)$. By differentiation for l_i, we find these fractions to be maximal for l_i being maximal, and the maximal fraction is given by $(1 + k(p-2)r)/(k(p-1))$. In turn, this fraction is maximal for k being minimal. Hence, the $\|\mathfrak{p}\|$-exponents of $\Psi_{r,\mathfrak{p}}(s)$ are less than -1 at least for $s > (1 + 2(p-2)r)/(2(p-1))$. The distance of this abscissa to $\alpha_p(C_p^r)$ is given by

$$\alpha_p(C_p^r) - \frac{1 + 2(p-2)r}{2(p-1)} = \frac{1 + (p-1)r}{p} - \frac{1 + 2(p-2)r}{2(p-1)} = \frac{p + 2(r-1)}{2p(p-1)}.$$

Hence, we can choose ε in the range

$$\frac{1}{2p} < \varepsilon < \frac{1}{2(p-1)} + \frac{r-1}{p(p-1)} = \frac{p + 2(r-1)}{2p(p-1)},$$

as desired. □

Corollary 6.4. *The function $\Psi_r(s)$ has the value*

$$\Psi_r(\alpha_p(C_p^r)) = \prod_{\mathfrak{p}} \left(1 + \|\mathfrak{p}\|^{-r} \sum_{l=1}^{p-1} \|\mathfrak{p}\|^{l(r-1)/p} \right) \prod_{l=1}^{p-1} \left(1 - \|\mathfrak{p}\|^{-r} \|\mathfrak{p}\|^{l(r-1)/p} \right).$$

Proof. For $s = \alpha_p(C_p^r)$, the term $\|\mathfrak{p}\|^{-s} \|\mathfrak{p}\|^{l(r-s)}$ of the Euler factor $\Psi_{r,\mathfrak{p}}(s)$ is a $\|\mathfrak{p}\|$-power with exponent

$$-\frac{1 + (p-1)r}{p} + l\left(r - \frac{1 + (p-1)r}{p} \right) = \frac{r - 1 - pr}{p} + \frac{lpr - l - l(p-1)r}{p} = -r + \frac{(l+1)(r-1)}{p}.$$

This leads to the proposed value of $\Psi_r(s)$ by the substitution $l+1$ for l. □

Corollary 6.5. *For $p = 2$, we have*

$$\Phi_r(s) = \zeta_F(2s - r) \, \zeta_F(2s)^{-1}.$$

Proof. We easily verify $\Lambda_r(s) = \zeta_F(2s - r)$ and $\Psi_r(s) = \zeta_F(2s)^{-1}$ by definition. □

Proposition 6.6. *The function $\Lambda_r(s)$ has the following properties.*

(a) *Let $r = 1$. Then $\alpha_p(C_p) = 1$, and $\Lambda_1(s)$ is holomorphic for $\Re(s) > 1 - 1/p$ except for the set of poles*

$$\left\{ 1 + \frac{2\pi i}{\log(q)} \frac{j}{\ell} : 0 \leq j < \ell \right\} + \frac{2\pi i}{\log(q)} \mathbf{Z},$$

where ℓ is the least common multiple of $2, \ldots, p$. The periodic poles corresponding to $s = 1$ is of maximal order $\beta(F, C_p) = p - 1$. In case $p \neq 2$, every other pole has less order.

13

(b) *Let $r > 1$. Then $\Lambda_r(s)$ is holomorphic for $\Re(s) > \alpha_p(C_p^r) - \min\{1/p, (r-1)/(p^2-p)\}$ except for the set of poles*

$$\left\{\alpha_p(C_p^r) + \frac{2\pi i}{\log(q)}\frac{j}{p} : 0 \le j < p\right\} + \frac{2\pi i}{\log(q)}\mathbf{Z}.$$

Every pole has order $\beta(F, C_p^r) = 1$.

Proof. Since the poles of $\zeta_F(s)$ are given by the values of s with $q^s = 1$ and $q^s = q$ respectively, we see, that the poles of $\Lambda_r(s)$ are given by the values of s with $q^{ls} = q^{(l-1)r}$ and $q^{ls} = q^{1+(l-1)r}$ for $l = 2, \ldots, p$ respectively. Each of these poles has period $2\pi i/(\log(q)\, l)$. We can ignore the former poles, as they are out of the region of interest due to

$$\alpha_p(C_p^r) - \frac{(l-1)r}{l} = \frac{l + (p-l)r}{pl} \ge \frac{1}{p}.$$

For the latter poles, we obtain

$$\alpha_p(C_p^r) - \frac{1 + (l-1)r}{l} = \frac{(p-l)(r-1)}{lp}.$$

This distance is minimal for l being maximal, whence assertion (b) follows. For assertion (a), we have $r = 1$, and every pole of $\Lambda_1(s)$ in the region $\Re(s) > 1 - 1/p$ lies on the axis $\Re(s) = 1$. Since the poles of $\zeta_F(s)$ are simple, the order of any pole of $\Lambda_1(s)$ cannot exceed $p - 1$. Since $2\pi i/\log(q)$ is the meet of all periods $2\pi i/(\log(q)\, l)$, only the poles $s \in 1 + 2\pi i/\log(q)\,\mathbf{Z}$ have maximal order $p - 1$, if $p \ne 2$. □

Now, Theorem 1.1 is an easy consequence of the results above.

Proof of Theorem 1.1. By Proposition 6.6, we only have to show, that $\Psi(s) = \Phi(F, C_p^r; s)\Lambda_r(s)^{-1}$ is convergent for $\Re(s) > a$ with $a = \alpha_p(C_p^r) - 1/(2p)$. We have the formal equality

$$\Psi(s) = e_r\Psi_r(s) + \sum_{i=1}^{r-1} e_i\Phi_i(s)\Lambda_r(s)^{-1} + \Upsilon_r(s)\Lambda_r(s)^{-1}$$

in the region of convergence, and we shall see that the right hand side has convergence abscissa a. By Lemma 6.3, $\Psi_r(s)$ is convergent for $\Re(s) > a$, and so is $\Upsilon_r(s)$ by Lemma 6.1. Further, $\Phi_i(s)$ has convergence abscissa $\alpha_p(C_p^i)$, which do not exceed a for $i < r$ due to

$$\alpha_p(C_p^r) - \alpha_p(C_p^i) = \frac{(p-1)(r-i)}{p} > \frac{1}{2p}.$$

The zeros of $\Lambda_r(s)$ are located of the imaginary axes $\Re(s) = (1 + 2(l-1)r)/2l$ for $l = 2, \ldots, p$, by the theorem of Hasse-Weil. These fractions are maximal for l being maximal, whence $\Lambda_r(s)^{-1}$ has convergence abscissa $(1 + 2(p-1)r)/2p = a$. Therefore, $\Psi(s)$ has abscissa a, too. □

7. Distribution of conductors of Artin-Schreier extensions

This section deals with the proofs of Theorem 1.2, Addendum 1.3, and Addendum 1.4. We consider the Dirichlet series

$$\Phi(F, C_p^r; s) = \sum_{\mathrm{Gal}(E/F) \simeq C_p^r} \|\mathfrak{f}(E/F)\|^{-s} = \sum_{n \ge 0} c_n t^n$$

14

as power series in $t = q^{-s}$ with coefficients c_n. Then the counting function $C(F, C_p^r; X)$ coincides with coefficients sum of this series via

$$C(F, C_p^r; q^m) = \sum_{n=0}^{m} c_n.$$

Proof of Theorem 1.2. By Theorem 1.1, the power series expansion of $\Phi(F, C_p^r; s)$ in $t = q^{-s}$ has radius of convergence $R = q^{-\alpha_p(C_p^r)}$, and it is meromorphic continuable beyond its circle of convergence. By Proposition 6.6, the poles of the continuation are of the form $t = R\xi^{-j}$ for some root of unity ξ. We now obtain Theorem 1.2 from Theorem Appendix A.5. The constant $\gamma(F, C_p^r)$ is hereby a positive real number, since the coefficients c_n are nonnegative integers. $\square$

Formulas for $\gamma(F, C_p^r)$ can be obtained by Theorem Appendix A.5. If we have more than one pole on the circle of convergence with maximal order, we have to use assertion (b), which involves some tedious calculations. We shall compute $\gamma(F, C_p^r)$ for $p = 2$ or $r = 1$ only, as we have only one or two poles of interest in these cases. It is clear, that $C(F, C_p^r; X)$ only depends on the coefficient sum of $e_r \Phi_r(s)$. Let $f(t) = e_r \Phi_r(s)$, $g(t) = e_r \Psi_r(s)$, $h(t) = \Lambda_r(s)$, and $Z_F(t) = \zeta_F(s)$ be the corresponding power series expansions of the respective Dirichlet series. Further, let $L_F(t) = (1-t)(1-qt)Z_F(t)$ be the L-polynomial of F. Then we have $f(t) = g(t)h(t)$ and

$$h(t) = \prod_{l=2}^{p} \frac{L_F(q^{(l-1)r}t^l)}{(1 - q^{(l-1)r}t^l)(1 - q^{1+(l-1)r}t^l)}.$$

Before we start with the calculations of $\gamma(F, C_p^r)$, the following identities are provided.

Proposition 7.1. (a) *We have*
$$e_r = \prod_{i=0}^{r-1} \frac{p}{p^r - p^i} = \frac{|C_p^r|}{|\mathrm{Aut}(C_p^r)|}.$$

(b) *We have*
$$\frac{L_F(q^{-1})}{1 - q^{-1}} = \log(q)\,\zeta_F(1).$$

Proof. The first equation in assertion (a) is just the definition of e_r as given in Proposition 5.1, and the second one is easy to verify. Assertion (b) follows from $\lim_{s \to 1}(s-1)/(1 - q^{1-s}) = 1/\log(q)$. $\square$

Proof of Addendum 1.4. Let $p \neq 2$ and $r = 1$. By Proposition 6.6, $f(t) = g(t)h(t)$ has only one pole on the circle of convergence $|t| = R = q^{-1}$ of maximal order $b = p - 1$. Let $c = \lim_{t \to q^{-1}}(t - q^{-1})^{p-1}h(t)$ be the limit of $h(t)$ at this pole. Then we obtain

$$\gamma(F, C_p) = -\frac{q^{p-1}\,g(q^{-1})\,c}{(p-2)!\,(1 - q^{-1})\,\log(q^{-1})^{p-2}} = \frac{q^{p-1}\,g(q^{-1})\,c}{(p-2)!\,(1 - q^{-1})\,\log(q)^{p-2}}$$

by Theorem Appendix A.5 (c). Observe that the sign of this constant is positive, since p is an odd prime. Using Corollary 6.4 and Proposition 7.1 (a) helps to identify the corresponding factors of $g(q^{-1})$ in the proposed formula. Now, we only have to verify

$$c = \lim_{t \to q^{-1}}(t - q^{-1})^{p-1}\,h(t) = \left(\frac{\log(q)\,\zeta_F(1)}{q}\right)^{p-1}\frac{1}{p!}.$$

15

We obtain the factor $(\log(q)\,\zeta_F(1))^{p-1}$ from the limit of $\prod_{l=2}^p Z_F(q^{l-1}t^l)/(1-q^{l-1}t^l)$ for $t \to q^{-1}$ via assertion (b) of Proposition 7.1. Finally, we have

$$\lim_{t\to q^{-1}}(t-q^{-1})^{p-1}\prod_{l=2}^p\frac{1}{1-(qt)^l} = \lim_{t\to q^{-1}}\left(\frac{qt-1}{1-qt}\right)^{p-1}\prod_{l=2}^p\frac{1}{q\sum_{k=0}^{l-1}(qt)^k} = \frac{1}{q^{p-1}\,p!}.$$

Putting all together, we obtain the formula for $\gamma(F,C_p)$ as stated. $\qquad\square$

Proof of Addendum 1.3. Let $p=2$ and $r \geq 1$. Then $f(t) = e_r Z_F(q^r t^2)/Z_F(t^2)$ by Corollary 6.5. We have two simple poles on the circle of convergence $|t| = R = q^{-(1+r)/2}$, namely $t = \pm R$. A priori, we have two relevant asymptotic equivalence classes for $C(F,C_2^r;X)$ by Theorem Appendix A.5 (b), namely one for $X = q^m$ with m running over even integers, and the one for m running over odd integers. Note that we only have to prove, that one of these equivalence classes coincides with the proposed one, by the redefinition of asymptotic equivalence as declared at the beginning of the article. By Theorem Appendix A.5, we have

$$\gamma_e = \lim_{n\to\infty}\frac{C(F,C_2^r;q^{2n+e})}{R^{-(2n+e)}} = -\left(\frac{R^{-1}\operatorname{Res}_{t=R}(f(t))}{1-R} + \frac{(-R)^{-1}\operatorname{Res}_{t=-R}(f(t))}{1+R}(-1)^e\right)$$

for $e = 0,1$. The residues for $t = \pm R$ only differ in their sign, and we obtain

$$\operatorname{Res}_{t=\pm R}(f(t)) = \frac{e_r\,\log(q)\,\zeta_F(1)}{\zeta_F(r+1)\,2(\pm R)^{-1}}.$$

Now, the constant γ_e differs from the proposed formula of $\gamma(F,C_2^r)$ by the factor $((1+R)+(-1)^e(1-R))/2$, and we obtain $\gamma(F,C_2^r) = \gamma_0 = \gamma_1/R$. Hence, the proposed equivalence class for $C(F,C_2^r;X)$ is true for $X = q^{2n}$ as $n \to \infty$. $\qquad\square$

Appendix A. Tauberian theorem for power series

In this section, we seek accurate asymptotic formulas for the coefficients and coefficient sums of a power series $f(t) = \sum_{n\geq 0} c_n t^n$. We will follow the lead of Michael Rosen's proof for Theorem 17.4 on page 311 in [9], which shall be generalised with part (a) of Lemma Appendix A.2 and Theorem Appendix A.5 for the sake of completeness. For the purpose of the article at hand, we are more interested in the coefficient sums, especially the parts (b) and (c) in latter-mentioned theorem. As a general assumption for this appendix, let R be the radius of convergence with $0 < R < 1$, and let $f(t)$ be holomorphic continuable in $|t| \leq R + \varepsilon$ for some $\varepsilon > 0$ with exception for a discrete pole set P, which is contained in the circle of convergence $|t| = R$. Further, let $p_u((t-u)^{-1}) = \sum_{k=1}^b p_{u,k}(t-u)^{-k}$ be the principal part of the Laurent series of $f(t)$ for $t = u$, and let $p_{u,b} \neq 0$ for at least one pole $u \in P$.

Proposition Appendix A.1. *Let $g_n(t) = 1/t^{n+1}$ and $h_m(t) = \sum_{n=0}^m g_n(t)$, and let $g_n^{(l)}(t)$, $h_m^{(l)}(t)$ denote their respective l-th derivative. Then the following holds.*

(a) *For any integer $n \geq 0$, we have*

$$\frac{g_n^{(l)}(t)}{l!} = -(-t)^{-(l+1)}\binom{n+l}{l}t^{-n}.$$

16

(b) *For any integer $m \geq 0$, we have*

$$\frac{h_m^{(l)}(t)}{l!} = -(-t)^{-(l+1)} \sum_{n=0}^{m} \binom{n+l}{l} t^{-n}.$$

Proof. Assertion (a) follows from $g_n^{(l)}(t) = (-1)^l t^{-(n+l+1)} \prod_{i=1}^{l}(n+i)$. By adding from $n = 0$ up to $n = m$, we hence obtain assertion (b). $\qquad\square$

Lemma Appendix A.2. *Let $f(t) = \sum_{n \geq 0} c_n t^n$ be a power series with properties as given above.*

(a) *The coefficient c_n fulfils the asymptotic relation*

$$\left| c_n - \sum_{u \in P} \sum_{k=1}^{b} (-u)^{-k} p_{u,k} \binom{n+k-1}{k-1} u^{-n} \right| \in o\left(R^{-n}\right).$$

(b) *The coefficient sum $\sum_{n=0}^{m} c_n$ fulfils the asymptotic relation*

$$\left| \sum_{n=0}^{m} c_n - \sum_{u \in P} \sum_{k=1}^{b} (-u)^{-k} p_{u,k} \sum_{n=0}^{m} \binom{n+k-1}{k-1} u^{-n} \right| \in o\left(R^{-m}\right).$$

Proof. For $m \geq 0$, let $e_m(t) = g_m(t)$ or $e_m(t) = h_m(t)$. Let γ be an anticlockwise oriented circle path with winding number 1 and radius $R + \varepsilon$ for some $0 < \varepsilon < 1 - R$. By the residue theorem, we have

$$\mathrm{Res}_{t=0}(f(t)e_m(t)) + \sum_{u \in P} \mathrm{Res}_{t=u}(f(t)e_m(t)) = \frac{1}{2\pi i} \oint_{\gamma} f(t)e_m(t)\,dt.$$

The right hand side including the integral can be bounded by $(R+\varepsilon) \max_{\gamma}(f(t)) \max_{\gamma}(e_m(t))$. The former maximum of this product exists, since γ is compact, and the latter maximum is of the form $o\left(R^{-(m+1)}\right)$, since $R < R + \varepsilon < 1$. In particular, $h_m(t) = t^{-(m+1)}(1 - t^{m+1})/(1 - t)$ holds. Hence, we have

$$\left| \mathrm{Res}_{t=0}(f(t)e_m(t)) + \sum_{u \in P} \mathrm{Res}_{t=u}(f(t)e_m(t)) \right| \in o\left(R^{-m}\right). \qquad (A.1)$$

The residue for $t = 0$ is c_m in case of $e_m(t) = g_m(t)$, and $\sum_{n=0}^{m} c_n$ in case of $e_m(t) = h_m(t)$. Further, the residues for the poles $t = u \in P$ are of the form

$$\mathrm{Res}_{t=u}(f(t)e_m(t)) = \sum_{k-l=1} p_{u,k} \frac{e_m^{(l)}(u)}{l!} = \sum_{k=1}^{b} p_{u,k} \frac{e_m^{(k-1)}(u)}{(k-1)!},$$

where the summands are coefficient products of the Laurent series for $f(t)$ and the Taylor series for $e_m(t)$ in $t = u$ respectively. This leads to the proposed relations by formula (A.1) and Proposition Appendix A.1. $\qquad\square$

Proposition Appendix A.3. *We have the asymptotic relation*

$$\left| \sum_{n=0}^{m} \binom{n+l}{l} t^{-n} - \frac{1}{l!\,(1-t)} t^{-m} m^l \right| \in o\left(R^{-m} m^l\right)$$

for $t \in \mathbf{C}$ being fixed with $|t| = R$, and $m \to \infty$.

Proof. We have the algebraic relation

$$(1-T)^{l+1} \sum_{n=0}^{m} \binom{n+l}{l} T^n = 1 - \sum_{i=0}^{l} \binom{m+i}{i} (1-T)^i T^{m+1},$$

a formula for the first m terms of the binomial series expansion for $(1-T)^{-(l+1)}$, which follows from induction over l. If we substitute T for a complex number z of absolute value $|z| = 1/R > 1$, we have

$$\sum_{n=0}^{m} \binom{n+l}{l} z^n = \frac{1}{(1-z)^{l+1}} - \sum_{i=0}^{l-1} \binom{m+i}{i} \frac{z}{(1-z)^{l+1-i}} z^m - \binom{m+l}{l} \frac{z}{1-z} z^m.$$

The binomial coefficient $\binom{n+i}{i}$ is a polynomial in n of degree i with leading coefficient $1/i!$. By subtracting the leading term of the right hand side, we obtain

$$\left| \sum_{n=0}^{m} \binom{n+l}{l} z^n + \frac{m^l}{l!} \frac{z}{1-z} z^m \right| \leq c\, R^{-m}\, m^{l-1},$$

where c is a constant not depending on m. Now, the proposed bound follows with the choice $z = 1/t$ and $|t| = R < 1$. $\qquad\square$

Lemma Appendix A.4. *Let $f(t) = \sum_{n \geq 0} c_n t^n$ be a power series with properties as given above. Further, assume the pole set P to be of the form $P = \{R\xi^{-j} : 1 \leq j \leq \ell\}$ for a primitive ℓ-th root of unity $\xi \in \mathbf{C}$, and let $p_j = p_{u,b}$ for $u = R\xi^{-j}$. Then the following holds.*

(a) *The coefficient c_n fulfils the asymptotic relation*

$$\left| c_n - \left(\sum_{j=1}^{\ell} \frac{(-R\xi^{-j})^{-b}\, p_j}{(b-1)!} \xi^{jn} \right) R^{-n}\, n^{b-1} \right| \in o\left(R^{-n}\, n^{b-1} \right).$$

For $n \to \infty$ running over some arithmetic progression modulo ℓ, we obtain $c_n \in \Theta\left(R^{-n}\, n^{b-1} \right)$.

(b) *The coefficient sum $\sum_{n=0}^{m} c_n$ fulfils the asymptotic relation*

$$\left| \sum_{n=0}^{m} c_n - \left(\sum_{j=1}^{\ell} \frac{(-R\xi^{-j})^{-b}\, p_j}{(b-1)!\,(1-R\xi^{-j})} \xi^{jm} \right) R^{-m}\, m^{b-1} \right| \in o\left(R^{-m}\, m^{b-1} \right).$$

For $m \to \infty$ running over some arithmetic progression modulo ℓ, we obtain $\sum_{n=0}^{m} c_n \in \Theta\left(R^{-m}\, m^{b-1} \right)$.

Proof. The formulas are an easy consequence from Lemma Appendix A.2 and Proposition Appendix A.3. By independence of characters, the inner sum running over the index j is nonzero for at least one congruence class modulo ℓ. By considering only integers of the so given arithmetic progression, we yield the size of the coefficients and their sums respectively. $\qquad\square$

Theorem Appendix A.5. *Let $f(t) = \sum_{n \geq 0} c_n t^n$ with pole set P be given as in Lemma Appendix A.4.*

(a) *There is some integer $1 \leq e \leq \ell$, such that the coefficient c_n has the asymptotic equivalence class*

$$c_n \sim \left(-\sum_{j=1}^{\ell} \frac{(R\xi^{-j})^{-b}\, p_j}{(b-1)!\,\log(R)^{b-1}} \xi^{je} \right) X\, \log(X)^{b-1}$$

for $X = R^{-n}$ and $n \to \infty$ running over the arithmetic progression $n \equiv e \pmod{\ell}$.

(b) *There is some integer $1 \le e \le \ell$, such that the coefficient sum $\sum_{n=0}^{m} c_n$ has the asymptotic equivalence class*

$$\sum_{n=0}^{m} c_n \sim \left(-\sum_{j=1}^{\ell} \frac{(R\xi^{-j})^{-b} \, p_j}{(b-1)! \, (1 - R\xi^{-j}) \, \log(R)^{b-1}} \, \xi^{je} \right) X \, \log(X)^{b-1}$$

for $X = R^{-m}$ and $m \to \infty$ running over the arithmetic progression $m \equiv e \pmod{\ell}$.

(c) *Assume $p_{u,b} \ne 0$ for $u = R$ only. Then we have*

$$\sum_{n=0}^{m} c_n \sim \left(-\frac{R^{-b} \, p_{R,b}}{(b-1)! \, (1 - R) \, \log(R)^{b-1}} \right) X \, \log(X)^{b-1}$$

for $X = R^{-m}$ and $m \to \infty$.

Proof. This theorem is just a restatement of Lemma Appendix A.4 with regard of $n = -\log(R^{-n})/\log(R)$. □

References

[1] Cohen, H., Diaz y Diaz, F., Olivier, M., 2002. On the density of discriminants of cyclic extensions of prime degree. J. reine angew. Math. 550, 169-209.

[2] Ellenberg, J., Venkatesh, A., 2005. Counting extensions of function fields with specified Galois group and bounded discriminant. Geometric Methods in Algebra and Number Theory 235, 151-168.

[3] Fesenko, I., Vostokov, S., 2002. Local Fields and Their Extensions, 2nd edition. AMS.

[4] Heß, F., Pauli, M., Pauli, S., 2003. Computing the multiplicative group of residue class rings. Math. Comput. 72, 1531-1548.

[5] Huppert, B., 1967. Endliche Gruppen I. Springer Verlag.

[6] Klüners, J., 2005. A counter example to Malle's conjecture on the asymptotics of discriminants. C. R. Math. 340, 411-414.

[7] Malle, G., 2002. On the distribution of Galois groups. J. Number Theory 92, 315-329.

[8] Malle, G., 2004. On the distribution of Galois groups II. Exper. Math. 13, 129-135.

[9] Rosen, M., 2002. Number Theory in Function Fields. Springer Verlag.

[10] Stichtenoth, H., 2008. Algebraic Function Fields and Codes, 2nd edition. Springer Verlag.

[11] Türkelli, S., 2008. Connected components of Hurwitz schemes and Malle's conjecture. to appear, arXiv:0809.0951.

[12] Wright, D., 1989. Distribution of discriminants of abelian extensions. Proc. London Math. Soc. (3) 58, 17-50.